

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MICROSOFT CORPORATION,
Petitioner,

v.

PROXENSE, LLC,
Patent Owner.

IPR2024-00407
Patent 9,679,289 B1

Before THU A. DANG, DAVID C. McKONE, and
NORMAN H. BEAMER, *Administrative Patent Judges*.

DANG, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

Microsoft Corporation (“Petitioner”) filed a Petition requesting an *inter partes* review of claims 1–20 (the “challenged claims”) of U.S. Patent No. 9,679,289 B1 (Ex. 1001, “the ’289 patent”). Paper 2 (“Pet.”). Proxense, LLC (“Patent Owner”) filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

Under 37 C.F.R. § 42.4(a), the Board has authority to determine whether to institute an *inter partes* review. Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we grant Petitioner’s request and institute an *inter partes* review of all challenged claims.

B. Related Proceedings

Petitioner identifies the ’289 patent as the subject of *Proxense, LLC v. Microsoft Corporation*, No. 6.23-cv-00319 (W.D. Tex.) and *Proxense, LLC v. Google LLC et al.*, No. 6.23-cv-00320 (W.D. Tex.) (“the parallel district court litigations”). Pet. 94. Other patents in the family of the ’960 patent are challenged by a different petitioner in *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01438, Paper 1; and *Samsung Electronics America, Inc. v. Proxense, LLC*, IPR2021-01439, Paper 1. *Id.*

C. The ’289 Patent

The ’289 patent, titled “Hybrid Device Having a Personal Digital Key and Receiver-Decoder Circuit and Methods of Use,” issued on June 13, 2017, from Application No. 14/961,645, with a filing date of December 7, 2015. Ex. 1001, codes (54), (45), (21), (22). The ’289 patent provides a

hybrid device including a personal digital key (PDK) and a receiver-decoder circuit (RDC) that are coupled for communication with each other. *Id.* at code (57).

An illustration of the embodiment of the '289 patent's hybrid device is depicted in Figure 1, reproduced below:

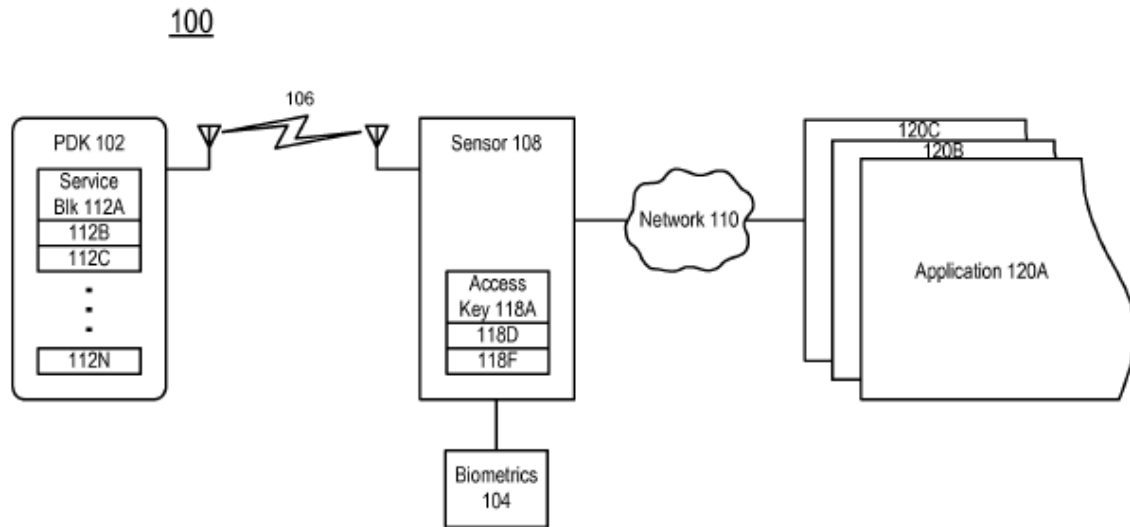


FIG. 1

Figure 1 is a block diagram of system 100 comprising PDK 102, sensor 108, network 110, and one or more applications 120 (including services). *Id.* at 3:27–31. In Figure 1, sensor 108 is coupled to PDK 102 by wireless link 106 and coupled to network 110 by a wired or wireless link. *Id.* at 3:31–33. In the exemplary embodiment shown in Figure 1, applications 120 are accessed over network 110, with sensor 108 being adapted to receive biometric input 104 from a user and displaying status to a user. *Id.* at 3:33–36.

In the example shown in Figure 1, sensor 108 contains three service block access keys 118A, 118D, 118F, wherein service block access keys 118 allow sensor 108 to unlock information stored in corresponding service

blocks 112, which information is used as local secured information. *Id.* at 3:43–50. In one example in which a biometric input is required in order to access specific service blocks in PDK 102, service block 112A is used for verification of the biometric input and sensor 108 uses stored corresponding service block access key 118A to unlock biometric service 112A. *Id.* at 3:51–56. A current biometric information is received using biometric input 104, and sensor 108 verifies the stored biometric input (from service block 112A) against the recently acquired biometric information (from input 104). *Id.* at 3:56–59.

An exemplary embodiment of sensor 108 is depicted in Figure 3, reproduced below:

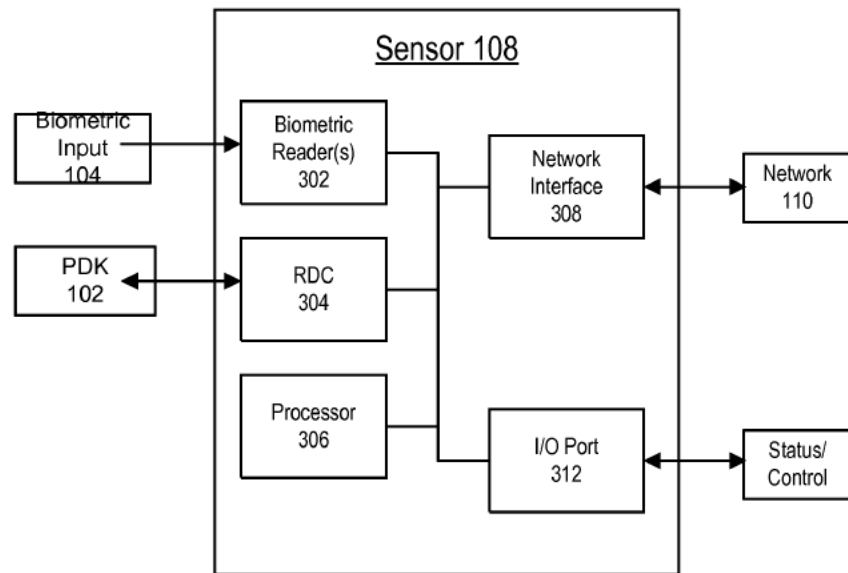


FIG. 3

Figure 3 is a block diagram of sensor 108 comprising one or more biometric readers 302, RDC 304, processor 306, network interface 308, and I/O port 312. *Id.* at 7:39–43. As shown in Figure 3, RDC 304 provides the wireless interface to PDK 102. *Id.* at 7:45–46.

Biometric reader 302 receives and processes biometric input 104 from an individual. *Id.* at 7:58–65. I/O port 312 provides general input and output interface to sensor 108. *Id.* at 8:10–17.

D. The Challenged Claims

Of the challenged claims, claims 1 and 14 are independent. Independent claim 1 is illustrative of the challenged claims, and is reproduced below:

1. A hybrid device comprising:

an integrated, secure memory storing local, secured information; and

an integrated reader-decoder circuit (RDC) for communicating wirelessly with at least one external device within a proximity zone, the integrated RDC communicatively coupled to the integrated, secure memory for communication with the integrated, secure memory,

wherein one or more of (a) the integrated RDC communicating wirelessly with the at least one external device within the proximity zone and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service.

Ex. 1001, 22:36–49.

E. Asserted Grounds of Unpatentability

Petitioner challenges the patentability of claims 1–20 of the '289 patent on the following grounds (Pet. 1–2):

Claim(s) Challenged	35 U.S.C. §¹	Reference(s)/Basis
1–20	103	Giobbi ’157 ² , Giobbi ’139 ³
1–20	103	Giobbi ’157, Giobbi ’139, Dua ⁴
1–8, 10, 11, 14–19	103	Broadcom ⁵
1–20	103	Broadcom, Giobbi ’157

Petitioner relies on the Declaration of Patrick Traynor, Ph.D.
(Ex. 1003) in support of its unpatentability contentions.

II. ANALYSIS

A. *Claim Construction*

We construe each claim “in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.” 37 C.F.R. § 42.100(b) (2020). Under this standard, claim terms are generally given their plain and ordinary meaning as would have been understood by a person

¹ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102, 103, effective March 16, 2013. Because the application from which the ’289 patent issued was a continuation of applications filed before this date, the pre-AIA versions of §§ 102, 103 apply.

² U.S. Patent Publication No. 2007/0245157 A1, published October 18, 2007, filed May 5, 2007 (Ex. 1005, “Giobbi ’157”).

³ U.S. Patent Publication No. 2004/0255139 A1, published December 16, 2004, filed May 17, 2004 (Ex. 1006, “Giobbi ’139”).

⁴ U.S. Patent No. 9,042,819 B2, issued May 26, 2015, filed September 30, 2014 (Ex. 1007, “Dua”).

⁵ European Patent Application No. EP 1,536,36 A1 published June 1, 2005, filed September 30, 2004 (Ex. 1008, “Broadcom”).

of ordinary skill in the art (POSITA) at the time of the invention and in the context of the entire patent disclosure. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc).

Only those terms in controversy need to be construed, and only to the extent necessary to resolve the controversy. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co. Matal*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

1. “hybrid device”

Patent Owner proposes construing “hybrid device” appearing in claims 1–16 and 19 as “a device comprising an integrated personal digital key (PDK) and an integrated receiver decoder circuit,” as “construed” by the district court in a case filed by Patent Owner against Samsung, *Proxense, LLC v. Samsung Electronics Co.*, 6:21-cv-00210-ADA (W.D. Tex.) (“Samsung case”). Prelim. Resp. 3–4 (citing Ex. 2001, 3 (construing claims of patents related to the ’289 patent, but not claims of the ’289 patent)). Petitioner provides its interpretation for “hybrid device” as “a device comprising an integrated, secure memory storing local, secured information and an integrated receiver-decoder circuit,” which, according to Petitioner, “is consistent with the use of the term in the specification of the ’289 patent.” Pet. 3–4. Petitioner explains that the district court’s construction “was predicated by the use of ‘PDK’ in the ‘hybrid device’ independent claims” of a “family member of the ’289 patent,” whereas “the ’289 patent does not recite the use of a ‘PDK’ in the ‘hybrid device’ independent claims.” *Id.*

The plain language of “hybrid device” does not suggest a requirement that it requires an integrated PDK. Nothing in the Specification clearly

limits or redefines “hybrid device” to a device comprising an integrated PDK, as Patent Owner proposes. Prelim. Resp. 3–4. Although Patent Owner contends that the district court construed “hybrid device” as “comprising an integrated personal digital key (PDK)” (*id.* (citing Ex. 2001, 3)), as Petitioner points out, the district court’s construction was predicated by the use of “PDK” in the “hybrid device” recited in the independent claims of a family member of the ’289 patent. Pet. 3–4. We agree with Petitioner that the ’289 patent does not recite that a “PDK” is part of the claimed “hybrid device.” *Id.* In fact, as Patent Owner acknowledges, except for dependent claim 20, the claims of the ’289 patent do not recite a PDK. Prelim. Resp. 8.

In view of the plain language of the claims and the Specification, we determine that the term “hybrid device” recited in claims 1–16, and 19 is not limited to “comprising an integrated personal digital key (PDK).” We determine no further explicit construction is necessary to resolve the parties’ issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

2. “receiver-decoder circuit (RDC)”

Patent Owner proposes construing “receiver-decoder circuit” appearing in claims 1, 3, 7, 14, and 16 as “a component or collection of components, capable of wirelessly receiving data in an encrypted format and decoding the encrypted data for processing” as “construed” by the district court in the Samsung case. Prelim. Resp. 7–8 (citing Ex. 2001, 4; Ex. 2004, 4). Petitioner contends that, “[f]or purposes of this proceeding, Petitioner adopts this construction [adopted in the district court].” Pet. 5. We determine no explicit construction of “receiver-decoder circuit” is necessary to resolve the parties’ issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

3. “*personal digital key (PDK)*”

Patent Owner points out that “[e]xcept for claim 20, the claims of the 289 Patent do not explicitly recite a ‘PDK.’” Prelim. Resp. 8. Nevertheless, Patent Owner contends that the district court in the Samsung case “construed” the term as “an operably connected collection of elements including an antenna and a transceiver for communicating with a RDC and a controller and memory for storing information particular to a user.” *Id.* (citing Ex. 2001, 3–4; Ex. 2004, 4). Petitioner contends that, “[f]or purposes of this proceeding, Petitioner adopts this construction of ‘personal digital key’ [adopted in the district court].” Pet. 4–5. We determine no explicit construction “personal digital key” is necessary to resolve the parties’ issues in controversy. *See Vivid Techs.*, 200 F.3d at 803.

4. “*local, secured information*”

Claim 1 recites “an integrated, secure memory *storing local, secured information.*” Ex. 1001, 22:37–38 (emphasis added). Claim 14 similarly recites this limitation. *Id.* at 24:6–7.

Patent Owner asserts that “the specification defines ‘local secured information’ as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.” Prelim. Resp. 27. Patent Owner cites to the Specification:

The PDK102 includes multiple service blocks 112A–N as described in more detail in FIG. 2. Each service block 112 is accessed using a corresponding service block access key 118. In this example, the sensor 108 contains three of the service block access keys 118A, D, F. ***The service block access keys 118 allow the sensor 108 to unlock information stored in the corresponding service blocks 112, which information is used as local secured information.***

Prelim. Resp. 27 (quoting Ex. 1001, 3:43–50). According to Patent Owner, this is “the only instance in the specification where the term ‘local secured information’ appears,” which “clearly defines ‘which information is used as *local secured information*.’” *Id.* at 28. Patent Owner contends that “[l]ocal, secured information’ is thus defined in the specification as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.” *Id.* at 29.

Petitioner does not propose a claim construction for “local, secured information” but relies on Giobbi ’157’s PDK for storing “biometric profile” in “tamper-proof” memory, and Broadcom’s authentication component 114 for storing “cryptographically secured” information on access device 102 or Broadcom’s integrated circuit 312 and data memory 314 for storing “encrypted keys used for authentication.” Pet. 28–29, 68–69 (citing Ex. 1005 ¶¶ 11, 27–28, 35, Figs. 2–3; Ex. 1008 ¶¶ 116–118, 125, Figs. 1, 3; Ex. 1003 ¶¶ 60, 111).

The plain meaning of “an integrated, secure memory storing local, secured information,” as claimed, suggests an integrated, secure memory for storing information locally, wherein the information is secured. *See* Pet. 28–29, 67–68; Prelim. Resp. 27–29. Further, nothing in the Specification clearly limits or redefines “local, secured information” to “information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK,” as Patent Owner proposes. Prelim. Resp. 27.

We are unpersuaded by Patent Owner’s contention that the Specification “clearly defines ‘which information is used as *local secured information*.’” Prelim. Resp. 28. Although Patent Owner points to an “instance” in the Specification that it alleges is such a “clear[] defin[ition],”

this portion of the Specification merely shows an exemplary embodiment and *not* a definition. *See* Ex. 1001, 3:43–50. The language Patent Owner points to in the Specification proves that “[i]n *this example*, the sensor 108 contains three of the service block access keys 118A, D, F,” wherein “[t]he service block access keys 118 allow the sensor 108 to unlock information stored in the corresponding service blocks 112, which information is used as local secured information.” Prelim. Resp. 28 (citing Ex. 1001, 3:43–50) (emphasis added). That is, although the referenced portion of the Specification indicates that, in an example, information stored in a “service block” can be used as “local secure information,” nothing in the Specification limits “local, secure information” to “information stored within service block of a PDK and unlocked with a corresponding access key provided to the PDK,” as Patent Owner contends.⁶ *Id.* Any special definition for “local, secured information” limiting it to “information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK” must be set forth in the Specification with reasonable clarity, deliberateness, and precision. *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). We do not discern such clarity, deliberateness, and precision to be present here.

In view of the plain language of the claims and the Specification, we determine that the term “local, secured information” as claimed

⁶ We are unpersuaded by Patent Owner’s contention that “the permissive language ‘in this example’ does not expand the definition ‘local secure information’” because “it applies to the sensors.” Prelim. Resp. 28. The Specification is clear that, in this example, “the” same service access keys 118 contained by the sensor allow the sensor to unlock information “used as local secured information.” *See* Ex. 1001, 3:43–50.

encompasses information stored locally on an integrated, secure memory, wherein the information is secured,,and is not limited to information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.

5. “*enabl[ing] one or more of an application, a function, and a service*”

Claim 1 recites a “one or more of (a) the integrated RDC . . . and (b) the local, secured information stored by the integrated, secure memory *enables one or more of an application, a function, and a service.*” Ex. 1001, 22:44–51 (emphasis added). Claim 14 similarly recites “enabling one or more of an application, a function and a service.” *Id.* at 24:10–11.

Patent Owner asserts that “[i]n response to arguments asserted in *Proxense v. Samsung* that the term ‘hybrid device’ was indefinite, the District Court found it necessary to construe the term ‘enabled.’” Prelim. Resp. 10–11. Patent Owner cites to the district court’s Memorandum in Support of Claim Construction Order:

An application, function, or service is ‘enabled’ by a PDK when it receives information from a PDK in exchange for an access key. Similarly, an RDC ‘enable[es] one or more of an application, a function, and a service’ when it forwards such a message to the application, function, or service. The claimed ‘hybrid device’ carries out these functions.

Prelim. Resp. 10–11 (citing Ex. 2002, 26). Patent Owner contends that Petitioner has not challenged this construction, and thus, “[u]nless compelled otherwise, this Board must ‘presume . . . that the same claim term in the same patent or related patents carries the same construed meaning.’” *Id.* at 4, 11 (citing *Omega Engineering, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003)).

We are unpersuaded by Patent Owner’s contention that “the District Court found it necessary to construe the term ‘enabled.’” Prelim. Resp. 10–11. In particular, we disagree that the district court in the Samsung case provided any construction for the term “enabled.” *Id.* Although Patent Owner points to the district court’s Memorandum in Support of Claim Construction Order (*Id.* (citing Ex. 2002, 26)) to support its contention that the district court construed the term “enabled,” this portion of the district court’s Memorandum merely discusses that “hybrid device” is not indefinite, and discusses exemplary operations of the “hybrid device” from which a POSITA “could reasonably ascertain the scope of the claim.” *See* Ex. 2002, 26. That is, a determination of whether a term is indefinite is not the same thing as construing a claim term. Thus, the district court’s determination that “hybrid device” is not indefinite did not construe that term, much less provide a construction of “enabled” recited in the claim. Accordingly, although the referenced portion of the district court’s Memorandum indicates that a POSITA could reasonably ascertain the scope of the claim (*id.*), nothing in the Memorandum provides a definition of “enabled” limited to “exchanging an access key for information held within a service block of a PDK,” as Patent Owner contends. Prelim. Resp. 24.

Patent Owner then contends that the ’289 patent “implicitly define[s] that ‘an application, function, or service is ‘enabled’ by a PDK when it receives information from a PDK in exchange for an access key.” Prelim. Resp. 18 (citing Ex. 2002, 26). Patent Owner references several examples in the Specification. *Id.* at 18–25 (citing Ex. 1001, 3:51–62, 8:55–65, 9:41–63, Figs. 1, 4–6). In particular, Patent Owner makes reference to Figure 6 of the ’289 patent:

In some cases, the first application 120Y1 is enabled from a first service block 112C, thus allowing a second application 120Y2 to operate using a second service block 112F (although the two applications need not be on the same device 510). For example, the first application 120Y1 might be the auto[]login/logoff, where a user logs into a personal computer via a service block 112C that provides a username and password.

Prelim. Resp. 18–19 (quoting Ex. 1001, 9:41–50) (emphasis omitted).

Patent Owner contends that, as shown in Figure 6, “credit card service 120Z1 is enabled by exchanging its access key 118A for the account data held within service block 112A to authorize a transaction.” *Id.* at 21.

Patent Owner contends that other “examples” of “enabling an application, a function or a service” presented in the Specification “also detail receiving information from a PDK in exchange for an access key.”

Prelim. Resp. 21. Patent Owner also references Figure 1 of the ’289 patent:

In one example, a biometric is required in order to access specific service blocks 112 in the PDK102. Verification of the biometric is achieved by using service block 112A. The sensor 108 stores the corresponding service block access key 118A and uses this key to unlock the biometric service block 112A, which stores a valid biometric. A current biometric is received using biometric input 104. The sensor 108 then verifies the stored biometric (from service block 112A) against the recently acquired biometric (from input 104). Upon proper verification, various applications 120 are permitted to connect to the PDK102 via the sensor 108 and/or to gain access to other service blocks 112.

Prelim. Resp. 21 (citing Ex. 1001, 3:51–62) (emphasis omitted).

“Consistent with the requirement that an application, function, or service is ‘enabled’ by a PDK when it receives information from a PDK in exchange for an access key,” Patent Owner then references Figure 4 of the ’289 patent:

An example of a local application (FIG. 4) is an auto login/logoff of a personal computer. When a PDK 102 is within the proximity of the personal computer 510, the PDK 102 is detected and the [s]ensor 108 attaches to the PDK 102 (using service block 112A). The login/logoff application 120 then sends the service block access key 118B along with a request for the contents of the service block 112B to the PDK 102 via the sensor 108. For example, a standard may specify that particular service block 112B contains username and password. These are returned to the application 120, allowing automatic login to the personal computer 510.

Prelim. Resp. 22–23 (quoting Ex. 1001, 8:55–65).

With “others,” Patent Owner references Figure 5 of the ’289 Patent:

An example of a remote application (FIG.5) is a credit card transaction. The sensor 108 in this case could be a credit card terminal. When the PDK 102 is brought in close proximity, the credit card terminal 108 attaches to the PDK 102 (using service block 112A). The terminal 108 then sends the PDK ID 212 to the credit card issuer (the external service) for identification. The credit card issuer may then send a service block access key 118B back to the sensor 108, where it is passed on to the PDK 102 to unlock a specific service block 112B. The contents of the service block 112B could then be sent back to the credit card issuer where further decryption could occur and the credit cardholder could be verified. Once verified, the credit card terminal displays that the transaction is approved.

Prelim. Resp. 23–24 (quoting Ex. 1001, 8:66–9:12).

Petitioner does not propose a claim construction for “enabl[ing] one or more of an application, a function, and a service” but relies on Giobbi ’157’s “transaction” which “includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.),” and Broadcom’s “method for providing access to a secured service,” wherein, once proximity is authenticated, “the user may then be allowed to access the secured service.” Pet. 34–37, 72–73 (citing

Ex. 1005 ¶¶ 11, 59–63, 65, Fig. 4; Ex. 1008 ¶¶ 10, 111–117, 119–120, 123–125; Ex. 1003 ¶¶ 65–68, 113).

The plain language of enabling an application, function, or service does not suggest a requirement that information be received from a PDK in exchange for an access key. Nothing in the Specification clearly limits the integrated, secure memory “enabl[ing] one or more of an application a function, and a service” to “receiv[ing] information from a PDK in exchange for an access key,” as Patent Owner proposes. Prelim. Resp. 18–25. Thus, we determine that “enabl[ing] one or more of an application a function, and a service” does not require receiving information from a PDK in exchange for an access key. *Id.*

We are unpersuaded by Patent Owner’s contention that the Specification implicitly defines “enabl[ing] one or more of an application a function, and a service” as requiring receiving information from a PDK in exchange for an access key. Prelim. Resp. 18–25. As Patent Owner acknowledged, “the specification may define claim terms by implication such that the meaning may be *found in or ascertained by* a reading of the patent documents.” *Id.* at 17 (citing *Trustees of Columbia Univ. v. Symantec*, 811 F.3d 1359, 1363–64 (Fed. Cir. 2016) (emphasis added)). Here, Patent Owner points to no portions in the Specification that provide the requisite reasonable clarity, deliberateness, and precision to warrant interpreting the claim language at issue as requiring “receiving information from a PDK in exchange for an access key.” *Id.* at 18–25.

Although Patent Owner points to Figures 1 and 4–6 of the Specification for such implicit definition, as Patent Owner acknowledges, Figures 1 and 4–6 of the Specification merely show various “examples” of “enabling an application, a function or a service” presented in the

Specification. Prelim. Resp. 21. In particular, the language in the Specification that Patent Owner points to with respect to Figure 6 provides “[i]n some cases, the first application 120Y1 is *enabled* from a first service block 112C,” wherein “[f]or example, the first application 120Y1 *might be* the *auto login/logoff*, where a user logs into a personal computer via a service block 112C that provides a username and password.”⁷ See Ex. 1001, 9:41–63 (emphases added). With respect to Figure 1, such teaching in the Specification shows that “[i]n one example, a biometric is required in order to access specific service blocks 112.” See *id.* at 3:51–62 (emphases added). With respect to Figure 5, such teaching in the Specification shows that “[a]n example of a remote application [] is a credit card transaction,” wherein “[t]he credit card issuer *may then send* a service block access key [] back to the sensor,” and “[t]he contents of the service block [] *could then be sent back* to the credit card issuer.” *Id.* at 8:66–9:12 (emphases added). With respect to Figure 1, such teaching in the Specification shows that “[a]n example of a local application (FIG. 4) is an *auto login/logoff* of a personal computer,” wherein, “[f]or example, a standard *may specify* that particular service block 112B contains username and password.” See *id.* at 8:55–65 (emphases added).

Although the referenced portions of the Specification discuss various examples wherein information may be received to “enable” various applications, functions, or services, nothing in these referenced portions of

⁷ Although Patent Owner contends that the phrase “[i]n some cases” . . . references the ability of a device to have more than one application enabled by a service block” (Prelim. Resp. 20), this portion of the Specification is clear that, in some (not all) cases, a first application, for example, an auto login/logoff, is enabled from a first service block. See Ex. 1001, 9:41–50.

the Specification clearly requires the “enabl[ing] an application, a function or a service” to only be by “receiv[ing] information from a PDK in exchange for an access key,” as Patent Owner contends. Prelim. Resp. 18–25. That is, Patent Owner points to no special definition, implicit or explicit, for “enabl[ing] an application, a function or a service” limiting it to “receiv[ing] information from a PDK in exchange for an access key” that is set forth in the Specification with reasonable *clarity, deliberateness, and precision*. *In re Paulsen*, 30 F.3d at 1480.

In view of the plain language of the claims and the Specification, we determine that the term “enabl[ing] an application, a function, and a service” recited in claims 1 and 14 is not limited to receiving information from a PDK in exchange for an access key. We determine no further explicit construction is necessary to resolve the controversy. *See Vivid Techs.*, 200 F.3d at 803.

B. Principles of Law

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, “would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art;

(3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness.⁸ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

C. Claims 1–20 as Obvious over Giobbi '157, Giobbi '139, and Dua

Petitioner contends that claims 1–20 of the '289 patent would have been obvious over by Giobbi '157, Giobbi '139, and alternatively, over Giobbi '157, Giobbi '139, and Dua. Pet. 7–61. In response, Patent Owner contends that the Petition fails to establish that Giobbi '157, Giobbi '139, and Dua “render the challenged claims invalid and unpatentable.” Prelim. Resp. 29–35.

We briefly summarize Giobbi '157, Giobbi '139, and Dua below.

1. Giobbi '157

Giobbi '157, titled “Two-Level Authentication for Secure Transaction,” published on October 18, 2007, with a filing date of May 5, 2007. Ex. 1005, codes (54), (43), (22). Giobbi '157 discloses a PDK that stores biometric profiles in “a tamper-proof memory that is acquired in a secure trusted process,” wherein the biometric profiles comprise a “representation of physical or behavioral characteristics that are uniquely associated with an individual that owns and carries the PDK.” *Id.* at code (57). An illustration of Giobbi '157's system for securely authenticating an individual for transaction processing and/or access control applications is depicted in Figure 1, reproduced below.

⁸ Neither party presents evidence or arguments regarding objective evidence of non-obviousness in the instant proceeding at this time.

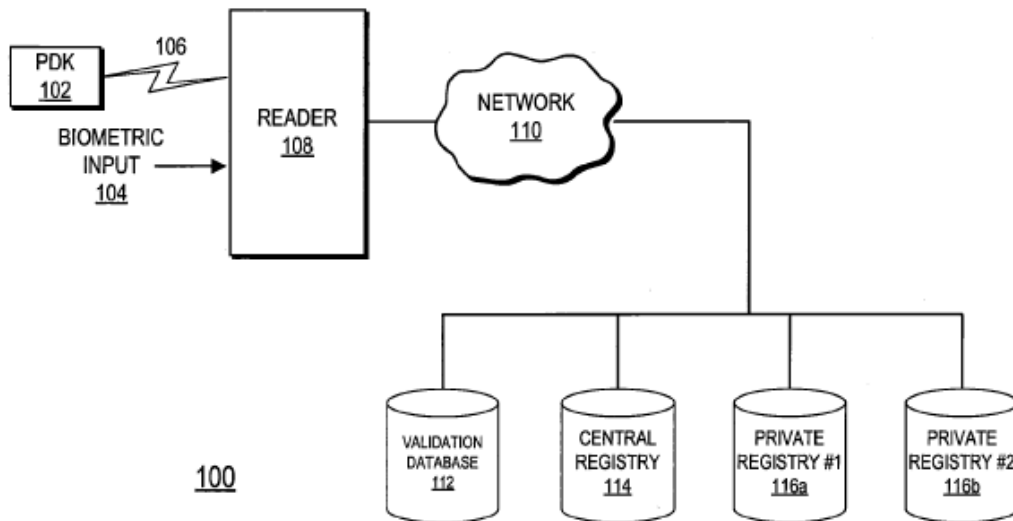


FIG. 1

Figure 1 is a block diagram of system 100 for secure electronic authentication comprising PDK 102, reader 108, network 110, and one or more external databases including validation database 112. *Id.* ¶ 26. As shown in Figure 1, reader 108 is coupled to PDK 102 by wireless link 106 and coupled to network 110 by either a wired or wireless link. *Id.* Reader 108 is also adapted to receive biometric input 104 from a user. Network 110 couples validation database 112, central registry 114, and two private registries 116 to reader 108. *Id.*

Reader 108 is depicted in Figure 3, reproduced below.

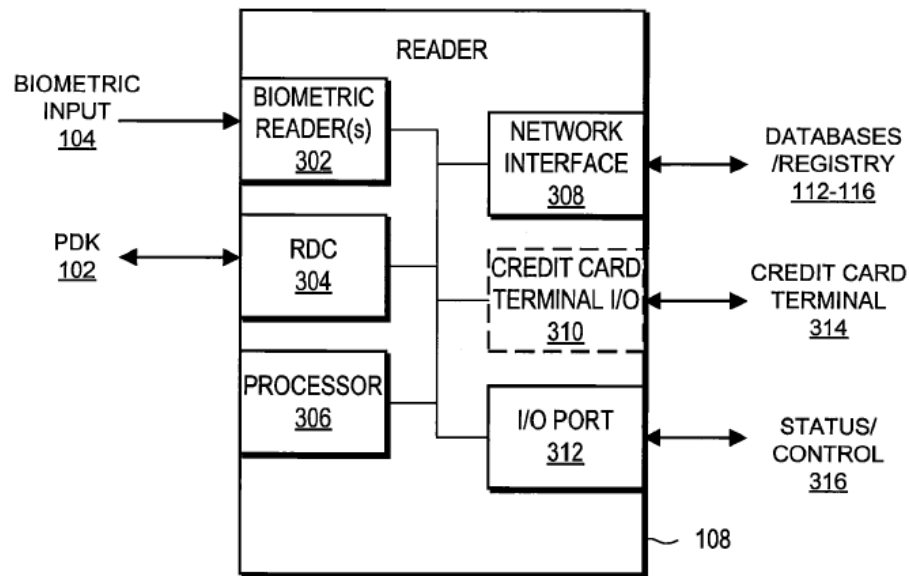


FIG. 3

Figure 3 is a block diagram of reader 108 that includes one or more biometric readers 302, receiver-decoder circuit (RDC) 304, processor 306, network interface 308, I/O port 312, and optionally credit card terminal I/O 310. *Id.* ¶ 49. As shown in Figure 3, RDC 304 provides wireless interface to PDK 102, wherein RDC 304 wireless receives data from PDK 102 in an encrypted format and decodes the encrypted data for processing by processor 306. *Id.* ¶ 50. Generally, processor 306 processes data received by reader 108 or data to be transmitted by reader 108, wherein biometric input 104 received by biometric reader 302 can be processed and compared to biometric profile 220 received from PDK 102 in order to determine if a transaction should be authorized. *Id.* ¶ 52.

PDK 102 is depicted in Figure 2, reproduced below.

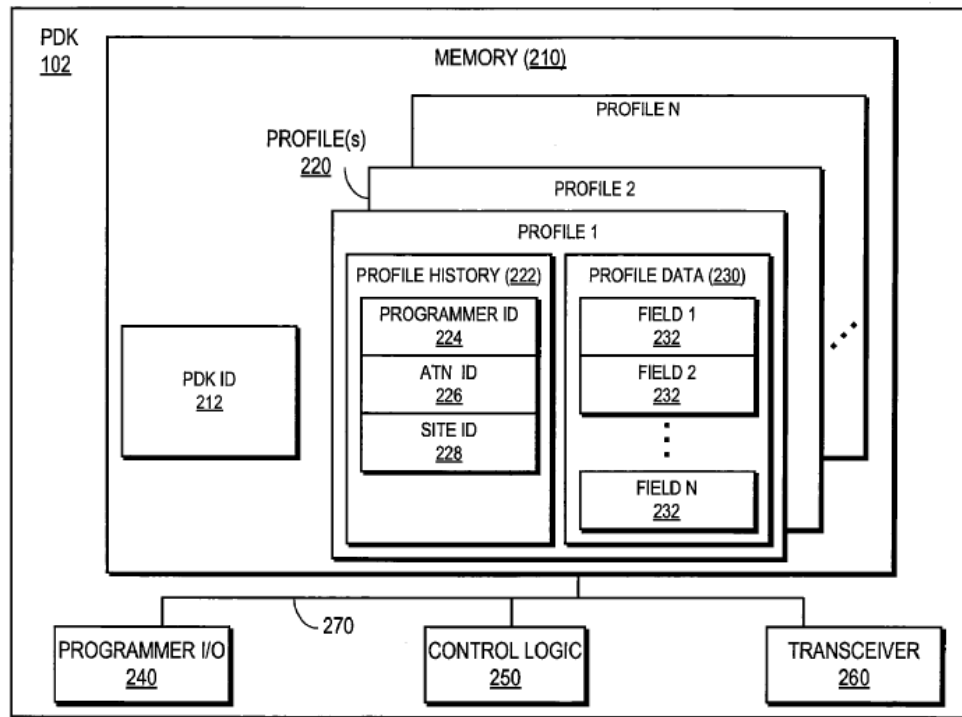


FIG. 2

Figure 2 is a block diagram of PDK 102 comprising memory 210, programmer I/O 240, control logic 250, and transceiver 260, coupled by bus 270. *Id.* ¶ 35. Memory 210 can be any combination of memory types, including physical access secured and tamperproof memories, that stores unique PDK ID 212 and one or more profiles 220. *Id.* ¶ 36. Profiles 220 may comprise a biometric profile, for example, which includes profile data 230 representing physical and/or behavioral information that can uniquely identify the PDK owner. *Id.* ¶ 37.

2. Giobbi '139

Giobbi '139, titled "Digital Content Security System," published on December 16, 2004, with a filing date of May 17, 2004. Ex. 1006, codes (54), (43), (22). Giobbi '139 discloses a personal digital key digital content security system (PDK-DCSS) that is used to protect computers from unauthorized use and protect the digital content stored on computers from

being wrongfully accessed and copied. *Id.* at code (57). Components of the PDK-DCSS are (1) a standard hard drive device, with the addition of a PDK receiver/decoder circuit (PDK-RDC) integrated into the hard drive's controller, and (2) a PDK key associated with the PDK-RDC. *Id.*

3. Dua

Dua, titled “Method, System, and Apparatus Having Near Field Communication (NFC) Chip With Configurable Memory That Is Updatable Via a Host Processor,” issued on May 26, 2015, with a filing date of September 30, 2014. Ex. 1006, codes (54), (45), (22). Dua discloses the use of Radio Frequency Identification (RFID) technology to exchange communication settings, media capability, and other parameters with an external device that also has integrated RFID technology. *Id.* at code (57). In particular, Dua discloses a media player with cellular phone capability. *Id.* at 6:46–65, Fig. 1. An RFID tag-reader module is attached to or embedded within the media player, wherein the RFID tag-reader module is capable of functioning as both an RFID tag and an RFID reader, and allows interoperability with readers and tags compatible with existing international standards. *Id.* at 12:46–56. Compatibility with these standards gives the media player the ability to not only establish a wireless connection with other electronic devices using RFID for setup, but also allows the media player to function as an electronic key and wallet (for point-of-sale transactions). *Id.* at 12:56–61.

4. Analysis of Claims 1–20 as being Obvious over Giobbi '157, Giobbi '139, and Dua

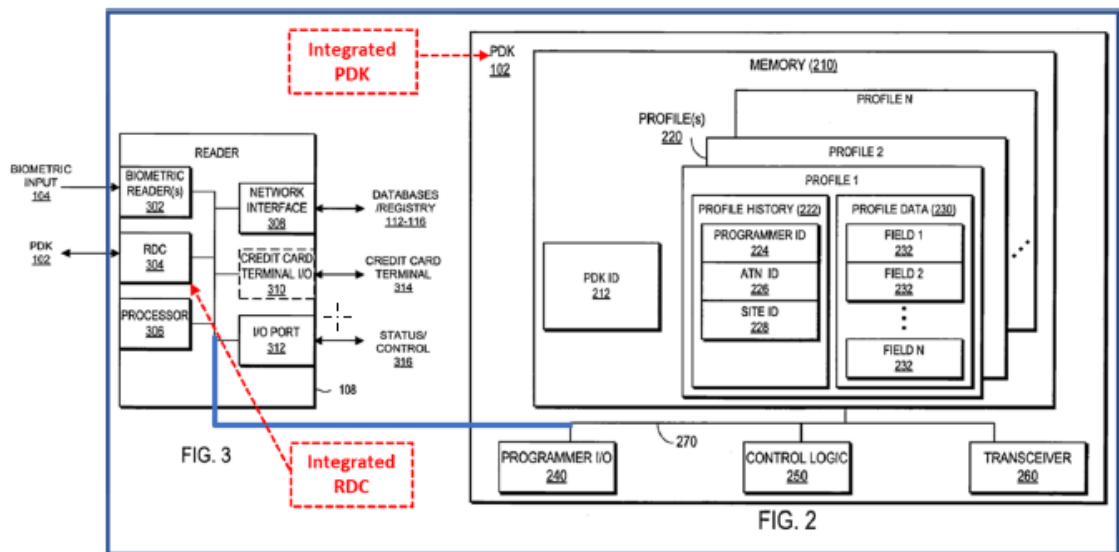
Petitioner contends that the claims of the '289 patent are directed to a “hybrid device” that “includes a personal digital key (PDK) and a receiver-decoder circuit (RDC).” Pet. 6. Petitioner contends that Giobbi '157

similarly teaches an “integrated PDK” that “can communicate [wirelessly] with [an external] receiver-decoder circuit (RDC).” *Id.* at 8.

i. Preamble, a “hybrid device” (claim 1)

Petitioner contends that, “[t]o the extent that the preamble is limiting, the combination of Giobbi -157 and-139 discloses a ‘**hybrid device**.’”

Pet. 26 (citing Ex. 1005 ¶¶ 12, 27, 30, 35; Ex. 1006 ¶¶ 22–44; Ex. 1003 ¶ 58). Petitioner provides an annotated combination of Figures 2 and 3 of Giobbi ’157, modified to incorporate Giobbi ’139’s teachings, shown below, to illustrate its contentions.



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).

The above annotated combination of Figures 2–3 of Giobbi ’157, according to Petitioner, illustrates “Giobbi-157’s cell phone” which “includes an integrated PDK” (top dotted red box) and in the combination of Giobbi ’157 and Giobbi ’139, “this integrated PDK communicates with an integrated RDC” (bottom dotted red box). Pet. 26–27 (citing Ex. 1005, Figs. 2–3; Ex. 1003 ¶ 58–59).

At this stage of the proceeding, Patent Owner does not present arguments in the Preliminary Response addressing the specific merits of

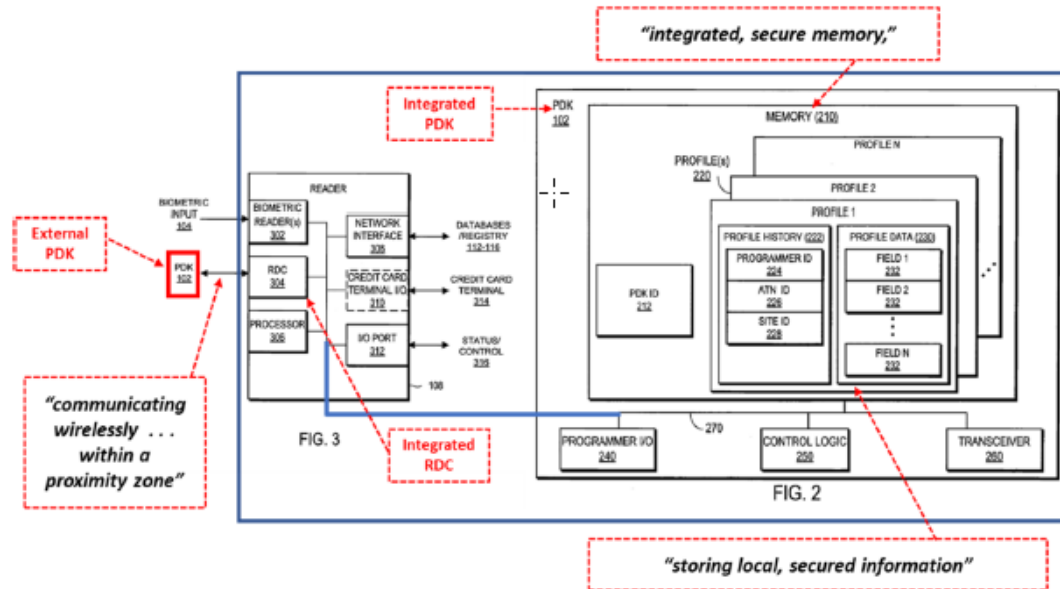
Petitioner's contentions with respect to the preamble. *See generally* Prelim. Resp. 29–32.⁹

Having reviewed all of Petitioner's assertions regarding this claim limitation, as well as the supporting evidence, we determine on this record that Petitioner has established a reasonable likelihood of establishing that the combination of Giobbi '157, Giobbi '139, and Dua teaches a “hybrid device.”

ii. “*an integrated, secure memory storing local, secured information*” (claim 1)

Petitioner contends that “Giobbi-157 discloses a ‘Personal Digital Key (PDK),’” wherein the PDK “is *integrated* into a hybrid device, such as a cell phone” and “stores one or more profiles (e.g., a biometric profile) [‘*secured information*’] in a tamper-proof [‘*secure*’] memory.” Pet. 28–29 (citing Ex. 1005 ¶¶ 11, 35). According to Petitioner, “Giobbi-157’s PDK stores information in *local* storage as the PDK is integrated into the hybrid device.” *Id.* at 29 (citing Ex. 1005 ¶¶ 11, 27–28; Ex. 1003 ¶ 60). Thus, Petitioner contends that “the device of the Giobbi-157-Giobbi-139 combination includes an ‘*integrated, secure memory*,’” as claimed. *Id.* Petitioner provides an annotated combination of Figures 2–3 of Giobbi '157, modified to incorporate Giobbi '139's teachings, shown below, to illustrate its contentions.

⁹ Because there is no dispute that Giobbi '157 in view of Giobbi '139 and Dua teaches a hybrid device, as recited in the preamble, for purposes of institution, we need not decide whether the preamble is limiting. *See Nidec*, 868 F.3d at 1017 (noting that “we need only construe terms ‘that are in controversy’” (quoting *Vivid*, 200 F.3d at 803)).



MS-1005, FIGS. 2-3 (modified to incorporate Giobbi-139’s teachings).

The above annotated combination of Figures 2–3 of Giobbi ’157, according to Petitioner, is modified to incorporate Giobbi ’139 to illustrate a PDK that stores secured information in a secure memory. Pet. 28–29. As shown in annotated Figures 2–3, memory 210 in PDK 102 is indicated as “integrated, secure memory” (top dotted red box) for “**storing local, secured information**” (bottom dotted red box). *Id.* at 29.

Petitioner further contends “Dua uses an RFID system to secure data and applications on its hybrid device” and the “RFID setup may act as an ‘electronic key’ for point-of-sale transactions and uses an RFID Tag as an electronic ‘key’ and an RFID Reader as the electronic ‘lock.’” Pet. 29–30 (citing Ex. 1007, 6:46–65, 12:51–64, 13:9–18, 14:53–64, 15:42–56, 16:31–34; Figs. 4A, 6). According to Petitioner “Dua’s RFID Tag Unit 306 is another example of an ‘**an integrated, secure memory storing local, secured information.**’” *Id.* at 30 (citing Ex. 1003 ¶ 61).

Patent Owner argues that the claimed “local, secured information” is “information stored within a service block of a PDK and unlocked with a

corresponding access key provided to the PDK.” Prelim. Resp. 29.

Although Patent Owner acknowledges that Giobbi ’157 discloses “a ‘portable device, referred to herein as a Personal Digital Key or “PDK”, [that] stores one or more profiles . . . in a tamper-proof memory,” Patent Owner contends that “Giobbi ’157 does not disclose or suggest that [the] tamper proof memory can include storing information within a service block of the PDK that is unlocked with a corresponding access key provided to the PDK.” *Id.* at 29–30 (citing Pet. 28–29; Ex. 1005 ¶¶ 11, 28, 36).

Patent Owner also contends that Dua merely discloses an RFID tag-reader module that allows interoperability with readers and tags compatible with existing international standards, but does not explain how the existing international standards provide an “electronic key” or how such key “can be provided by storing information locally within a service block of the RFID tag, which information is unlocked with a corresponding access key provided to the RFID tag.” Prelim. Resp. 30 (citing Ex. 1007, 12:52–61). According to Patent Owner, although Dua discloses “information stored in RFID tag unit 306 that can be retrieved by an RFID reader device [that] is stored in memory” and “[a]ccess to the configurable tag memory may be limited to one or more specific applications,” the “access control” in Dua is not “accomplished by providing an access key to the RFID tag to unlock stored information.” *Id.* at 31 (citing Ex. 1007, 14:53–57, 15:42–56).

Although Patent Owner acknowledges that the “memory components in RFID Tag-Reader Module 113 may be tamper resistant” for preventing hackers “from retrieving confidential information and encryption keys,” Patent Owner contends that Dua fails to disclose that “tamper proofing is accomplished by storing confidential information or encryption key, ‘locally,’ meaning within a service block of a RFID tag and unlocked with a

corresponding access key provided to the RFID tag.” *Id.* at 31 (citing Ex. 1007, 16:31–34).

We find Patent Owner’s arguments unavailing. In particular, as Petitioner points out, Giobbi ’157 discloses a PDK integrated into a device, such as a cell phone that stores a biometric profile, i.e., “secured information,” in a tamper-proof memory. Pet. 28; *see* Ex. 1005 ¶¶ 11, 35. Patent Owner acknowledges that Giobbi ’157 discloses “a ‘portable device, referred to herein as a Personal Digital Key or “PDK”, [that] stores one or more profiles . . . in a tamper-proof memory.’” Prelim. Resp. 29 (citing Ex. 1005 ¶ 11). Thus, we find persuasive Petitioner’s reliance on Giobbi ’157’s PDK, which locally stores digital information in a tamper-proof format, for teaching an integrated, secure memory for storing information locally, wherein the information is secured. Pet. 28–29; *see also* Ex. 1005 ¶ 28.

In our claim construction section above, we gave “an integrated, secure memory storing local, secured information” its ordinary and customary meaning as an integrated, secure memory for storing information locally, wherein the information is secured. In particular, we determine that an interpretation of “local, secured information” encompasses information stored locally on an integrated, secure memory, but is not limited to information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.

We also find Patent Owner’s arguments regarding Dua (Prelim. Resp. 30–31) unavailing, as they similarly rely on an interpretation of “local, secured information” that is not required by the aforementioned construction. In particular, as Patent Owner acknowledges, Dua discloses “information stored in RFID tag unit 306 that can be retrieved by an RFID

reader device [that] is stored in memory” and “[a]ccess to the configurable tag memory may be limited to one or more specific applications.” *Id.* (citing Ex. 1007, 14:53–57, 15:42–56). That is, Patent Owner does not contest Petitioner’s assertion that “Dua’s RFID Tag Unit 306 is another example of an ‘an integrated, secure memory storing local, secured information’” (Pet. 30 (citing Ex. 1003 ¶ 61) (emphasis omitted)), but merely contends that Dua fails to disclose “storing confidential information or encryption keys ‘locally,’ meaning within a service block of a RFID tag and unlocked with a corresponding access key provided to the RFID tag” (Prelim. Resp. 31), which is not required by our construction *supra*.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that the combination of Giobbi ’157 in view of Giobbi ’139 and Dua teaches “an integrated, secure memory storing local, secured information,” as recited in claim 1.

- iii. “wherein one or more of (a) the integrated, wireless communication interface . . . and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service” (claim 1)

Petitioner contends that Giobbi ’157 discloses “[w]hen a PDK [] comes within range of a Reader [], communication is automatically established [] between the RDC . . . and the PDK . . . when it enters a proximity zone of the [RDC].” Pet. 34 (citing Ex. 1005 ¶¶ 59–63). According to Petitioner, Giobbi ’157 then provides for the RDC requesting profile data stored within the external PDK for authentication, and if the profile data received from the “secure memory” of the external PDK is valid, the RDC “completes the transaction,” wherein a “transaction” includes “enabling access to secure physical or digital assets,” i.e., “***enables one or more of an application, a function, and service.***” *Id.* (citing Ex. 1005 ¶¶ 61, 63; Ex. 1003 ¶ 65).

Petitioner provides an annotated Figure 4 of Giobbi ’157, shown below, to illustrate its contentions.

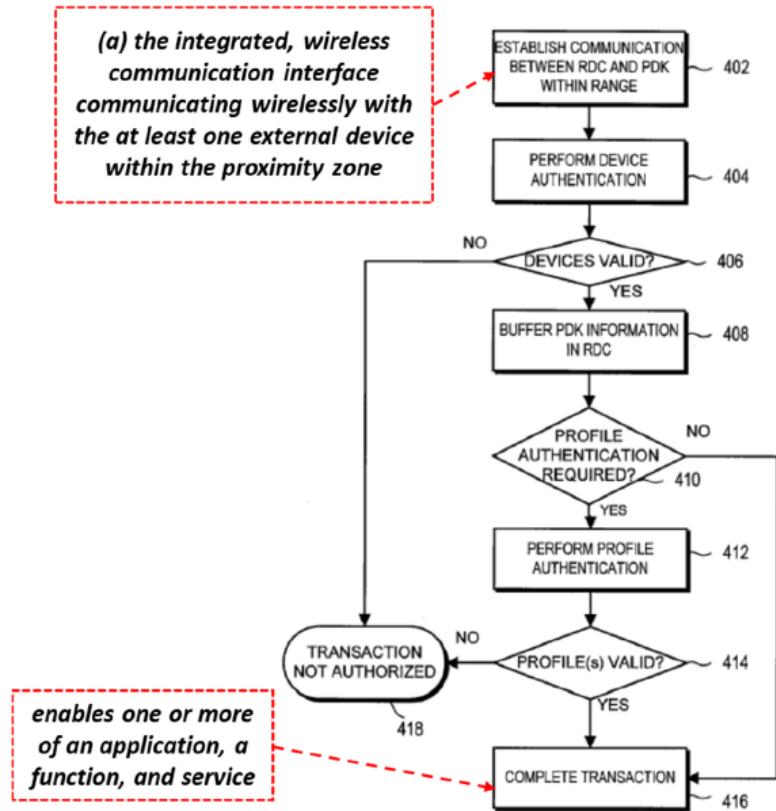


FIG. 4

MS-1005, FIG. 4.

The above annotated Figure 4 of Giobbi '157, as discussed in the Petition, illustrates a block diagram illustrating a method for establishing communication between an RDC and a PDK within range. Pet. 35. In annotated Figure 4 of Giobbi '157, the method begins with “the integrated, wireless communication interface communicating wirelessly with [] at least one external device within the proximity zone” (top dotted red box), wherein, upon transaction completion 416, the method “enables one or more of an application, a function and a service” (bottom dotted red box). Pet. 34–35 (citing Ex. 1005 ¶¶ 59–63, 65) (emphasis omitted).

According to Petitioner, Giobbi '157 “explicitly” teaches that the transaction “enables one or more of an application, a function, and service”

when stating that “the transaction includes enabling access to secure physical or digital assets (e.g., unlocking a door, opening a vault, providing access to a secured hard drive, etc.).” Pet. 37 (citing Ex. 1005 ¶ 63; Ex. 1003 ¶ 67) (emphasis omitted).

Petitioner also contends, alternatively, that “the integrated secure memory” of the hybrid device in Giobbi ’157 “enables one or more of an application, a function, and service” using “the local, secured information stored by the integrated, secure memory.” *Id.* at 35–36 (citing Ex. 1005, code (57), ¶ 11) (emphasis omitted). According to Petitioner, transactions in Giobbi ’157 are performed by transmitting authenticating information from the integrated PDK (“***integrated, secure memory***”) to a reader (a RDC), for example, when completing a withdrawal from an ATM. *Id.* (citing Ex. 1005 ¶ 65; Ex. 1003 ¶ 66).

In addition, Petitioner contends Giobbi ’139 discloses a use case where an integrated RDC can be incorporated into cell phones, PDAs, and MP3 players. Pet. 37 (citing Ex. 1006 ¶ 88). According to Petitioner, in Giobbi ’139 “[i]f an authorized PDK (***integrated, secure memory***) is used in conjunction with the integrated RDC the application/function/service runs on the hybrid device,” e.g., “the device ‘plays the digital content,’ such as music (***enables one or more of an application, a function, and service***).” *Id.* (citing Ex. 1006 ¶ 37; Ex. 1003 ¶ 68).

Patent Owner responds that the exchanged information referenced by the Petitioner in Giobbi ’157 is not “received in exchange for an access key provided to the PDK.” Prelim. Resp. 32. According to Patent Owner, Giobbi ’157 does not teach or suggest that “this unsecure[d] exchange of information can be accomplished by providing an access key in exchange for information held locally in the PDK’s service blocks as required by the

challenged claims.” *Id.* at 33. Patent Owner contends the second exchange in Giobbi ’157 likewise does not disclose providing an access key. *Id.* at 33–34. In particular, according to Patent Owner, “while the PDK may send a message containing various account information, Giobbi ’157 fails to describe or otherwise teach unlocking such information from a service block using an access key as required by the challenged claims.” *Id.* at 34. Patent Owner contends that “Giobbi ’139 also fails to disclose that the ‘activation code’ is provided in exchange for an access key provided by the playing device.” *Id.* Accordingly, Patent Owner contends that “neither Giobbi ’157 nor Giobbi ’139 disclose . . . ‘enabling one or more of an application, a function, and a service.’” *Id.* at 34–35.

We find Patent Owner’s arguments unavailing. In particular Patent Owner is relying on a claim construction of “enabling” requiring “providing an access key in exchange for information held locally in the PDK’s service blocks” (Prelim. Resp. 32–35) that is not required by our construction discussed above. As discussed above, we determine that the term “enabl[ing] an application, a function or a service” is not limited to “receiv[ing] information from a PDK in exchange for an access key.”

Giobbi ’157 teaches, for example, a RDC requesting profile data stored within the external PDK for authentication, wherein, if the profile data received from the external PDK is valid, the RDC completes the transaction, which includes enabling access to secure physical or digital assets. *See* Ex. 1005 ¶¶ 61, 63, Fig. 4. We are persuaded by Petitioner’s reliance on Giobbi ’157’s “transaction” wherein its completion “enabl[es] access to secure physical or digital assets,” i.e., “***enables one or more of an application, a function, and service.***” *See* Pet. 35.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that the combination of Giobbi '157 in view of Giobbi '139 and Dua teaches “one or more of (a) the integrated, wireless communication interface . . . and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service,” as recited in claim 1.

iv. Remaining limitations of claim 1

Petitioner provides detailed explanations as to how the combination of Giobbi '157, Giobbi '139, and Dua teaches the remaining claim limitations as recited in independent claim 1, citing Dr. Traynor's testimony for support. Pet. 30–33 (citing Ex. 1005 ¶¶ 12, 26–44, 50, Fig. 3; Ex. 1006 ¶¶ 22–44; Ex. 1007, 6:46–65, 12:51–64, 13:9–18, 14:53–64, 15:42–46, 16:31–34, Figs. 4A, 6; Ex. 1003 ¶¶ 62–64). For example, Petitioner contends that Giobbi '157's RDC receives data from the PDK, and discloses “[t]he Reader 108 wirelessly communicates with the PDK 102 when the PDK 102 is within a proximity zone of the Reader 108.” *Id.* at 30–31 (citing Ex. 1005 ¶¶ 26–44, 50). Petitioner further contends that Dua's Reader Unit is another example of an “integrated, wireless communication interface,” as “Reader Unit 304 also ‘*communicat[es] wirelessly with at least one external device within a proximity zone*’ and is ‘*communicatively coupled to [an] integrated, secure memory*’ (the RFID Tag Unit 306).” *Id.* at 31–33 (citing Ex. 1007, 6:46–65, 12:51–64, 13:9–18, 14:53–64, 15:42–56, 16:31–34, Figs. 4A, 6; Ex. 1003 ¶ 64).

At this stage in the proceeding, Patent Owner does not address separately Petitioner's explanations and supporting evidence regarding the remaining limitations in claim 1. *See generally* Prelim. Resp.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that independent claim 1 would have been obvious over Giobbi '157, Giobbi '139, and Dua.

v. *Claims 2–20 as Obvious over Giobbi '157, Giobbi '139, and Dua*

Petitioner provides detailed explanations as to how the combination of Giobbi '157, Giobbi '139, and Dua renders the limitations as recited in claims 2–20 obvious, citing Dr. Traynor's testimony for support. Pet. 37–61 (citing Ex. 1005, code (57), ¶¶ 9, 11–13, 26–43, 47–53, 55, 59–63, 65–67, 74, Figs. 1–4, 7D; Ex. 1006 ¶¶ 67–69, 87–91; Ex. 1007, 8:20–29; Ex. 1003 ¶¶ 69–104). At this stage in the proceeding, Patent Owner does not address separately these explanations and supporting evidence by Petitioner regarding claims 2–20. *See generally* Prelim. Resp.

Having reviewed Petitioner's arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claims 2–20 would have been obvious over the combination of Giobbi '157, Giobbi '139, and Dua.

5. *Analysis of Claims 1–20 as Obvious over Giobbi '157 and Giobbi '139*

Petitioner contends that claims 1–20 of the '289 patent would also have been obvious over just Giobbi '157 and Giobbi '139, but provides the same arguments discussed above for the obviousness ground over Giobbi '157, Giobbi '139, and Dua. Pet. 7–61. Patent Owner responds with the same arguments discussed above for the obviousness ground based on Giobbi '157, Giobbi '139, and Dua. Prelim. Resp. 28–32. Thus, at this stage of the proceeding, we do not separately address Petitioner's

obviousness ground based on Giobbi '157 and Giobbi '139. Nonetheless, Patent Owner may raise arguments regarding this obviousness ground in the Response after institution.

E. Claims 1–20 as obvious over Broadcom and over Broadcom and Giobbi '157

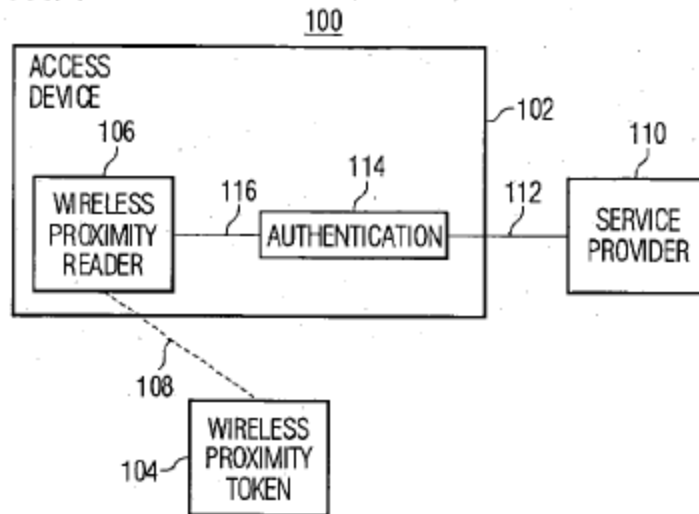
Alternatively, Petitioner contends that claims 1–8, 10, 11, and 14–19 of the '289 patent also would have been obvious over Broadcom (Pet. 61–84), and that claims 1–20 of the '289 patent would have been obvious over Broadcom in view of Giobbi '157. *Id.* at 89. In response, Patent Owner contends that Petitioner fails to demonstrate that Broadcom discloses or renders obvious the claim limitations. Prelim. Resp. 35–38.

We briefly summarize Broadcom below.

1. Broadcom

Broadcom, titled “Proximity Authentication System,” published on June 1, 2005, with a filing date of September 30, 2004. Ex. 1008, codes (54), (43), (22). Broadcom discloses controlling access to secured services based on the proximity of a wireless token to a computing device through which access to the secured services is obtained, wherein an authorized user is provided access to a service only when the wireless token assigned to the user is in the proximity of the computing device. *Id.* at code (57). A user’s credential may be stored on the token and a reader may be implemented within a security boundary on the computing device, and thus, the credential may be passed to the security boundary without passing through the computing device via software messages or applications. *Id.* An illustration of Broadcom’s proximity-based authentication system is depicted in Figure 1, reproduced below.

FIG 1



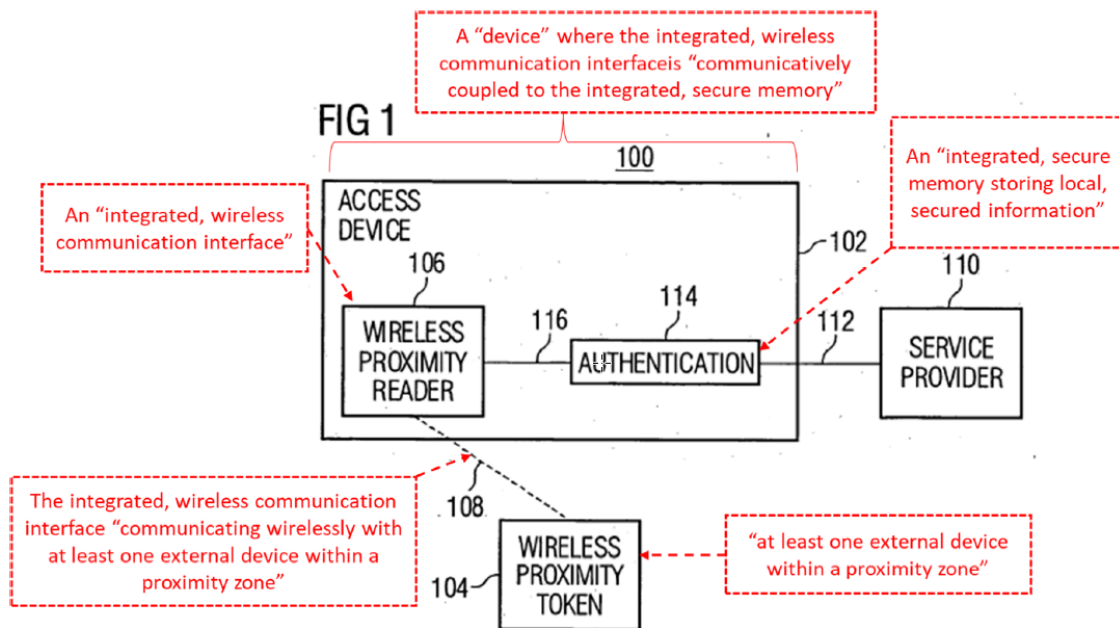
Broadcom's Figure 1 is a block diagram of system 100 comprising access device 102 used to determine whether wireless token 104 assigned to a user or users is proximate to access device 102. *Id.* ¶¶ 110–111. As shown in Figure 1, wireless proximity reader 106 is configured to receive signals 108 from wireless proximity token 104, wherein signals 108 includes information that uniquely identifies wireless proximity token 104 and includes credentials (e.g., a password) that may be used to access a secured service provided by service provider 110. *Id.* ¶ 111.

2. Analysis of Claims 1–8, 10, 11, and 14–19 as Obvious over Broadcom

Petitioner contends that Broadcom teaches “a system for secured access to a service based on a wireless device coming within[] the proximity of a reader,” wherein a user's credentials are stored on an RFID token and this token and associated authentication credentials are then read by an RFID reader. Pet. 61 (citing Ex. 1008, code (57), ¶¶ 9–16, Ex. 1003 ¶ 105). In particular, according to Petitioner, the Access Device including the reader authenticates the RFID token and permits access to the secured service after

authentication. *Id.* According to Petitioner, Broadcom teaches storing authentication information securely within memory that is tamper resistant and not exposed in the mobile device. *Id.* at 63 (citing Ex. 1008 ¶¶ 13, 134, 167, 187, 192; Ex. 1003 ¶ 106).

Petitioner provides an annotated Figure 1 of Broadcom, shown below, to illustrate its contentions.



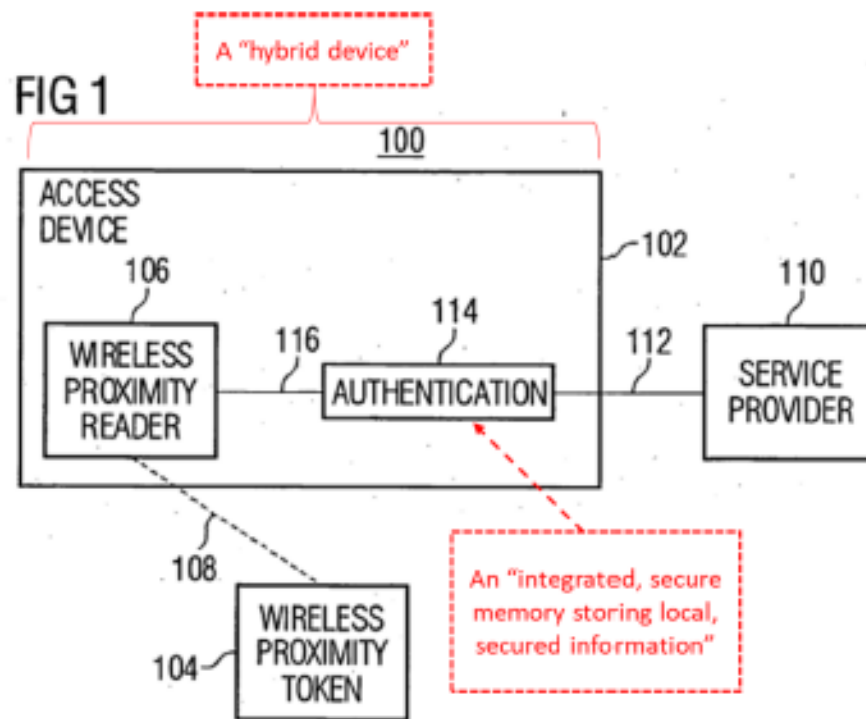
MS-1008, FIG. 1 (annotated).

The above annotated Figure 1 of Broadcom in the Petition illustrates access device 102, which requests access to service provider 110 and “verif[ies] that the information sent from the token 104 includes a credential associated with an authorized user and/or access device.” Pet. 62–63 (citing Ex. 1008 ¶¶ 113–119 130, 181; Ex. 1003 ¶ 107). As shown in annotated Figure 1, wireless proximity token (104) is wirelessly connected (108) to wireless proximity reader (106). *Id.* at 62.

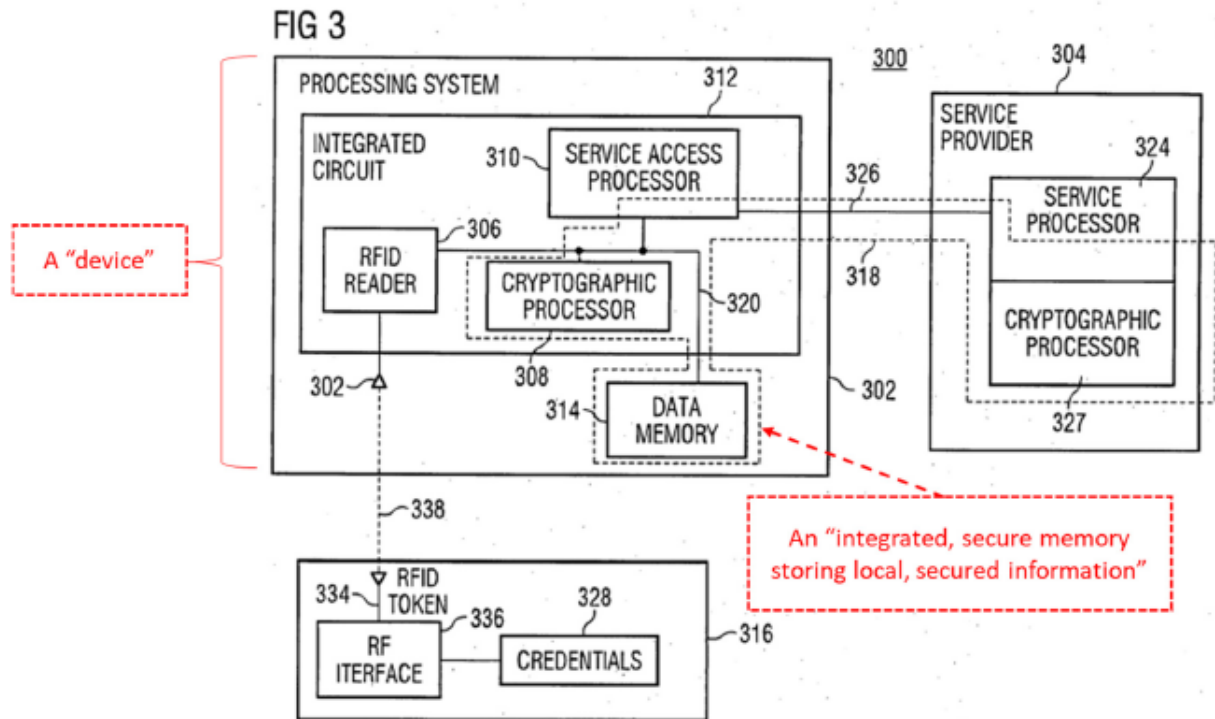
- i. “an integrated, secure memory storing local, secured information” (claim 1)

Petitioner contends that “Broadcom’s ‘authentication component 114’ stores information locally on the access device 102 and is ‘cryptographically secured’ (‘**an integrated, secure memory**’).” Pet. 68 (citing Ex. 1008 ¶¶ 116–118, Fig. 1). Petitioner contends that “Broadcom discloses an ‘integrated circuit 312’ and a ‘data memory 314’ (‘**an integrated, secure memory**’) to store encrypted keys used for authentication (‘**local, secured information**’).” *Id.* (citing Ex. 1008 ¶¶ 135–137, Fig. 3).

Petitioner provides annotated Figures 1 and 3 of Broadcom, shown below, to illustrate its contentions.



MS-1008, FIG. 1.



MS-1008, FIG. 3.

Annotated Figures 1 and 3 of Broadcom, as discussed in the Petition, illustrate “components within Broadcom’s access device (‘*an integrated, secure memory*’), which can be a ‘a personal computer, a server, a cellular phone, a personal data assistant (‘PDA’).” Pet. 68–69 (citing Ex. 1008 ¶ 125, Figs. 1–3; Ex. 1003 ¶ 111). As shown in annotated Figure 1, authentication component 114 is indicated as “[a]n ‘integrated, secure memory storing local, secured information’” (bottom dotted red box). *Id.* at 69. As shown in annotated Figure 3, data memory 314 is indicated as “[a]n ‘integrated, secure memory storing local, secured information’” (right dotted red box). *Id.*

Patent Owner replies that Broadcom’s “‘data memory 314’ is not unlocked by an access key provided by the service provider as required by the challenged claim(s).” Prelim. Resp. 35. In particular, Patent Owner

repeats the argument that “the specification defines ‘local, secured information’ as information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK.” *Id.* According to Patent Owner, Broadcom “only discloses the use of a key ***provided by a PDK*** to decrypt information received from data memory 314.” *Id.*

We find Patent Owner’s arguments unavailing. As Patent Owner acknowledges, Petitioner relies on Broadcom’s “data memory 314” storing the claimed “local, secured information” (Prelim. Resp. 35), wherein Petitioner contends that data memory 314 stores encrypted information used for authentication (Pet. 68). In fact, Patent Owner does not contest Petitioner’s reliance on Broadcom for teaching a PDK for storing encrypted information. Prelim. Resp. 35.

As discussed above, an interpretation of “local, secured information” as “information stored within a service block of a PDK and unlocked with a corresponding access key provided to the PDK,” as Patent Owner asserts, (Prelim. Resp. 35) is not required by the aforementioned construction.

We find persuasive Petitioner’s reliance on Broadcom’s “‘data memory 314’ (***an integrated, secure memory***)” to store “encrypted keys used for authentication (***local, secured information***).” Pet. 68; *see also* Ex. 1008 ¶¶ 135–137, Fig. 3. Furthermore, Petitioner relies on, which Patent Owner does not address, Broadcom’s “authentication component 114” that stores information locally “on the access device 102 and is ‘cryptographically secured’ (***an integrated, secure memory***).” Pet. 68; *see also* Ex. 1008 ¶¶ 116–118, Fig. 1.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that Broadcom teaches “an integrated, secure memory storing local, secured information,” as recited in claim 1.

- ii. “wherein one or more of (a) the integrated, wireless communication interface . . . and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service” (claim 1)

Petitioner contends that Broadcom discloses that “the access device 102 may automatically request a predefined service once the user places the token 104 (*‘at least one external device’*) proximate the access device 102” using “a wireless proximity reader 106 [*‘integrated RDC’*] . . . configured to receive signals 108 (e.g., RF signals) from the wireless proximity token 104.” Pet. 72 (citing Ex. 1008 ¶¶ 111–117). According to Petitioner, “[a]fter the token 104 has been brought within the proximity zone of the reader 106, ‘the service provider 110 may then enable access to the requested service’ (*‘enables of one or more of an application, a function, and a service’*).” *Id.* (citing Ex. 1008 ¶ 119).

According to Petitioner, Broadcom discloses “providing access to a secured service based on a user’s proximity.” Pet. 72–73. Petitioner contends that, in Broadcom, once the proximity is authenticated, the user may then “be allowed to access the secured service[] (*‘one or more of an application a function, and a service’*).” *Id.* at 73 (citing Ex. 1008 ¶ 8). Petitioner contends that Broadcom notes that “the term service may include, for example, access to data and/or a data processing service,” wherein:

a service may enable an access device to, for example, read or write data in a data memory, access encrypted data, use cryptographic keys, gain access to cryptographic material such

as security association and keys, access a web page, access a data network or access a processing application.

Pet. 73 (citing Ex. 1003 ¶ 113; quoting Ex. 1008 ¶ 120).

Patent Owner responds that Broadcom accesses services by way of an RFID token broadcasting credentials when activated by a reader, subsequently passed to a service provider for access. Prelim. Resp. 37. Although Patent Owner acknowledges that Broadcom “teaches sending messages containing credential information from a token activated by proximity,” Patent Owner contends that, “as the message is the result of the token being powered by an RF signal, the first message lacks information received from a token in exchange for an access key provided to the token.” *Id.* According to Patent Owner, “no key is provided in [the] exchange for the information.” *Id.*

We find Patent Owner’s arguments unavailing, because Patent Owner is again relying on a claim construction of “enabling,” requiring receiving information “from a token in exchange for an access key provided to the token” (Prelim. Resp. 36–38) that is not required by our construction discussed above. Thus, we are unpersuaded by Patent Owner’s contention that Broadcom fails to disclose the “enabling” limitation because “Broadcom . . . teaches sending messages containing credential information from a token activated by proximity.” *Id.* at 37.

Here, as Patent Owner acknowledges, Broadcom teaches sending messages containing credential information for access to a service. Prelim. Resp. 37. We agree with Petitioner’s reliance on Broadcom’s “providing access to a secured service based on a user’s proximity” for teaching “enabl[ing]” a service. Pet. 72–73; *see* Ex. 1008 ¶¶ 111–117, 119–120.

On this preliminary record, we are persuaded that Petitioner has made a sufficient showing that Broadcom teaches “one or more of (a) the integrated, wireless communication interface . . . and (b) the local, secured information stored by the integrated, secure memory enables one or more of an application, a function, and a service,” as recited in claim 1.

iii. Remaining limitations of claim 1, and claims 2–8, 10, 11, and 14–19

Petitioner provides detailed explanations as to how Broadcom teaches the remaining claim limitations as recited in independent claim 1, independent claim 14 reciting similar limitations, and claims 2–8, 10, 11, and 15–19 depending respectively therefrom, citing Dr. Traynor’s testimony for support. Pet. 70–71, 73–84 (citing Ex. 1008 ¶¶ 8–10, 12, 16, 110–120, 123, 127, 129–130, 133–138, 141, 148, 163–168, 193–196, Figs. 1–6; Ex. 1003 ¶¶ 112, 115–138). At this stage in the proceeding, Patent Owner does not address separately Petitioner’s explanations and supporting evidence regarding the remaining limitations in claim 1 and claims 2–8, 10, 11, and 14–19. *See generally* Prelim. Resp.

Having reviewed Petitioner’s arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that independent claim 1, independent claim 14 reciting similar limitations, and claims 2–8, 10, 11, and 15–19 depending respectively therefrom, would have been obvious over Broadcom.

**3. Analysis of Claims 1–20 as Obvious over
Broadcom and Giobbi ’157**

Petitioner provides detailed explanations as to how the combination of Broadcom and Giobbi ’157 teaches the limitations as recited in claims 1–20,

citing Dr. Traynor’s testimony for support. Pet. 84–89 (citing Ex. 1008 ¶¶ 113–119, 130, 136–139, 146; Ex. 1005 ¶¶ 11, 32–35, 53, 74; Ex. 1003 ¶¶ 139–148).

At this stage in the proceeding, Patent Owner does not address separately Petitioner’s explanations and supporting evidence regarding claims 1–20 over Broadcom and Giobbi ’157. *See* Prelim. Resp. 38–39. Rather, Patent Owner merely contends that “as noted *supra* with respect to [Broadcom only ground], the Petition has not established Broadcom discloses all elements of the challenged independent claims 1 and 14,” wherein, “because elements of the independent claims are not met,” the Petition “fails to establish that Broadcom or Giobbi ’157 or a combination thereof invalidate claims 1–20.” *Id.*

Having reviewed Petitioner’s arguments and supporting evidence in the present record, we determine Petitioner has demonstrated a reasonable likelihood that it will prevail on its assertion that claims 1–20 would have been obvious over Broadcom in further view of Giobbi ’157.

III. CONCLUSION

Because we determine that Petitioner has demonstrated a reasonable likelihood that it would prevail in showing at least one of the challenged claims is unpatentable, we institute *inter partes* review as to all challenged claims and grounds presented in the Petition. 37 C.F.R. § 42.108(a) (2020). At this stage of the proceeding, we have not made a final determination as to the patentability of any of these challenged claims.

IV. ORDER

For the reasons given, it is

ORDERED that pursuant to 35 U.S.C. § 314, an *inter partes* review is instituted as to claims 1–20 of the '289 patent to determine whether:

- 1) claims 1–20 are unpatentable under 35 U.S.C. § 103 as obvious over Giobbi '157, and Giobbi '139;
- 2) claims 1–20 are unpatentable under 35 U.S.C. § 103 as obvious over Giobbi '157, Giobbi '139, and Dua;
- 3) claims 1–8, 10, 11, and 14–19 are unpatentable under 35 U.S.C. § 103 as obvious over Broadcom;
- 4) claims 1–20 are unpatentable under 35 U.S.C. § 103 as obvious over Broadcom and Giobbi '157; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial, which commences on the entry date of this Decision.

IPR2024-00407
Patent 9,679,289 B1
For PETITIONER:

W. Karl Renner
Roberto Devoto
Jonathan Driesslein
Usman Khan
FISH & RICHARDSON P.C.
axf-ptab@fr.com
devoto@fr.com
driesslein@fr.com
khan@fr.com

For PATENT OWNER:

David Hecht
James Zak
HECHT PARTNERS LLP
dhecht@hechtpartners.com
jzak@hechtpartners.com